

## QUANTUM-RESISTANT CRYPTOGRAPHIC PROTOCOL ANALYSIS USING DEEP REINFORCEMENT LEARNING

Alfred Basta, PhD, LCCA, C|CISCO, CRISC, CISM, CISA, CGEIT, PMP, CHFI, ESCA\*<sup>1</sup>,

Rebecca Basta, CAP, PCAD, PMP, CIPP/US, AIGP, CDPPM, Six Sigma Master Black Belt\*<sup>2</sup>,

Stavros Basta, GISCP, LPTM, CPENT, GSLC, CISM, PMP, CIPP/US, CompTIA Security+\*<sup>3</sup>

\*<sup>1,2,3</sup>R & Amp;S Educational Consultants Inc.

DOI: <https://www.doi.org/10.56726/IRJMETs91621>

### ABSTRACT

Today's cryptographic algorithms maintain security through defense against multiple attack approaches, but advancing encryption protocols leads to advanced attack methods. A breakthrough cryptanalysis system based on reinforcement learning technology is presented in this research to detect weaknesses in cryptographic systems automatically. The proposed reinforcement learning system improves its attack methods through learning from previous tests and continuously becomes more proficient. Our team evaluates this methodology against blockchain ciphers like AES while testing public key usage like RSA. The model can discover sophisticated mistakes that resist detection with traditional cryptanalysis methods. The adaptable and expandable framework provides the foundation for future cryptography exploration and automated attack creation methods.

### I. INTRODUCTION

**Foundations: Deep Reinforcement Learning, Post-Quantum Cryptography, and Side-Channel Analysis**

#### Deep Reinforcement Learning in Security Applications

Deep Reinforcement Learning (DRL) has emerged as a transformative approach for addressing complex security challenges. (Cryptanalysis et al., 2025) presents a breakthrough reinforcement learning system designed to detect weaknesses in cryptographic systems automatically. The proposed approach improves its attack methods through learning from previous tests, demonstrating the capacity to discover sophisticated mistakes that resist detection with traditional cryptanalysis methods. This foundational work establishes DRL as a viable methodology for adaptive security testing in cryptographic protocols.

Beyond cryptographic analysis, DRL has shown remarkable effectiveness in automated vulnerability exploitation. (AlMajali et al., 2024) developed a deep reinforcement learning agent specifically configured to exploit targeted vulnerabilities through a training phase where the agent learns and stores payloads along with their corresponding reward values in a neural network. Their approach achieved a maximum accuracy of 96.6% in establishing reverse shells, demonstrating DRL's potential for automated security assessment.

#### Post-Quantum Cryptography Standards and Algorithms

The emergence of quantum computing has necessitated a paradigm shift in cryptographic standards. (Ezeogu, 2025) provides comprehensive implementation and performance analysis of the four NIST standard candidate post-quantum algorithms: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+, all tuned for high-throughput, low-latency applications. The research demonstrates that Kyber-1024 is best-suited for encryption tasks with minimal performance overhead (2.3x slower than AES-256), while Dilithium-5 offers the most efficient trade-off for long-term signature security.

(Rane, 2025) conducts a detailed comparative analysis of five primary categories of quantum-resistant cryptographic algorithms: lattice-based, code-based, hash-based, multivariate polynomial, and isogeny-based encryption schemes. Among these approaches, lattice-based cryptography has gained significant attention due to its robust security properties and computational efficiency, making it a strong candidate for standardization.

---

**Side-Channel Attacks: Threat Landscape**

Side-channel attacks represent one of the most critical threats to cryptographic implementations, exploiting physical leakage rather than algorithmic vulnerabilities. (Obaid & Alheeti, 2023) conducts a thorough examination of side-channel attacks, classifying diverse approaches including timing cryptanalysis, power-based cryptanalysis, video-based cryptanalysis, and memory-based cryptanalysis. The research demonstrates that understanding the subtleties of side-channel attacks is crucial to strengthening the security of cryptographic systems.

(Tosun et al., 2025) presents methods for conducting higher-order non-profiled side-channel attacks on lattice-based cryptography, covering both scenarios where device leakage is known and where it follows an unknown model. Their analysis of the NIST PQC standards Dilithium and Kyber achieved full secret-key recovery using only 700 and 2400 traces for second and third-order masked implementations, demonstrating the severity of implementation vulnerabilities.

**Traditional Cryptanalysis vs. AI-Driven Approaches**

Traditional cryptanalysis methods, while theoretically sound, often suffer from efficiency limitations when applied to complex cryptographic systems. (Kim et al., 2025) explores integrating machine learning knowledge to provide empirical evaluations of cryptosystems, proposing novel applications of ML algorithms that can be applied in known plaintext settings to perform cryptanalysis. Their approach correctly identifies encryption schemes that are not IND-CPA secure, such as DES, RSA, and AES ECB, with high accuracy, demonstrating that ML-based evaluation can serve as a quick sanity check complementary to traditional methods.

## **II. AUTOMATED VULNERABILITY DISCOVERY USING AI AND MACHINE LEARNING**

**Reinforcement Learning for Attack Pattern Discovery**

The automation of vulnerability discovery through reinforcement learning represents a paradigm shift in security testing. (McFadden et al., 2024) proposes WENDIGO, a black-box Deep Reinforcement Learning approach for discovering Denial-of-Service exploitable queries against GraphQL applications. The system builds increasingly complex queries while maximizing response time, demonstrating that DRL can effectively discover attack vectors using minimal requests—sometimes as few as two GraphQL requests per hour, compared to the high volume required by traditional DoS attacks.

(Hore et al., 2022) introduces Deep VULMAN, a deep reinforcement learning agent combined with integer programming to address cyber vulnerability management in resource-constrained environments. The sequential decision-making framework determines near-optimal resource allocation for mitigation and selects prioritized vulnerability instances for remediation, outperforming current deterministic methods on both simulated and real-world vulnerability data.

**Hardware-Based Vulnerability Testing and Detection**

(Chen et al., 2024) presents a deep reinforcement learning-based framework for automatic test case generation in hardware verification, incorporating a modified Deep Q-Network architecture with prioritized experience replay. The framework demonstrates significant improvements, achieving 17.2% coverage improvement and a 65% reduction in verification time compared to traditional approaches, with a 94.8% detection rate for security vulnerabilities in cryptographic hardware like AES cores.

(V et al., 2023) proposes a novel strategy combining Deep Q-Network (DQN), Proximal Policy Optimization (PPO), and Dueling Deep Q-Network (DDQN) algorithms for automated network vulnerability identification. The approach achieves 95% detection accuracy with incredibly low false positive (3%) and false negative (2%) rates, high precision (94%), recall (96%), low execution time (25 ms), and good scalability.

**Machine Learning-Based Cryptanalysis**

(Marin et al., 2025) introduces Physics-Informed Graph Neural Networks (PIGNN) for attack path prediction, achieving an F1 score of 0.9308 for full-path prediction. This novel architecture effectively captures adversarial

patterns in high-dimensional spaces, providing a scalable and automated approach to vulnerability assessment that complements manual security analysis.

(Kim et al., 2025) demonstrates how mutual information neural estimation can calculate a cryptosystem's mutual information leakage, and binary cross entropy classification can model indistinguishability under chosen plaintext attack (CPA). The research shows that ML-based cryptanalysis can identify vulnerabilities in cryptosystems more efficiently than exhaustive approaches, providing a practical methodology for rapid security evaluation.

### **Adaptive Testing Frameworks**

(Amouei et al., 2022) presents Reinforcement-Learning-Driven and Adaptive Testing (RAT), an automated black-box testing strategy to discover injection vulnerabilities in Web Application Firewalls. The methodology clusters similar attack samples together and utilizes reinforcement learning combined with a novel adaptive search algorithm, achieving 33.53% and 63.16% improvement on average compared to state-of-the-art methods in discovering bypassing payloads.

## **III. POST-QUANTUM CRYPTOGRAPHIC IMPLEMENTATION SECURITY**

### **Lattice-Based Cryptography Vulnerabilities**

Lattice-based cryptography forms the foundation of NIST's post-quantum standardization, yet implementations remain vulnerable to sophisticated attacks. (Kasture et al., 2025) evaluates side-channel vulnerabilities in CRYSTALS-Kyber through correlation and differential power analysis, revealing that unprotected FPGA implementations across all parameter sets were successfully compromised. Additive Boolean masking provided varying protection levels, with 4-bit masking offering a 100× security increase at notable performance cost.

(Qiao et al., 2025) proposes a hybrid SCA on Dilithium, leveraging both profiled and non-profiled attack strengths. Their method profiles a template using leakage from operations with known variables, then applies it to target sensitive variables, requiring only 10/27/18 power traces to recover keys for Dilithium2/3/5 respectively, significantly reducing trace requirements compared to prior non-profiled attacks.

### **Countermeasures and Protective Mechanisms**

(Ravi et al., 2023) presents a systematic study of side-channel and fault injection attacks on Kyber and Dilithium, along with customized countermeasures capable of providing simultaneous protection against several SCA- and FIA-based chosen-ciphertext attacks. The research demonstrates implementations on both ARM Cortex-M4 and Cortex-A53 processors, revealing that custom countermeasures incur reasonable performance overheads.

(Beirendonck et al., 2021) describes a side-channel-resistant implementation of Saber using masking as a countermeasure. The design proves very efficient to masking due to power-of-two moduli and limited noise sampling of learning with rounding, featuring only a 2.5x overhead factor for masked key decapsulation requiring less than 3,000,000 cycles on the Cortex-M4.

### **Hardware-Software Codesign Approaches**

(Fritzmman et al., 2021) proposes masked HW/SW codesigns of NIST PQC finalists Kyber and Saber, suitable for their different characteristics. The design presents a novel masked ciphertext compression algorithm for non-power-of-two moduli and develops a generic Number Theoretic Transform (NTT) multiplier efficient for schemes not based on NTT. Results show cycle counts of K:214k/E:298k/D:313k for Kyber with NIST Level III parameter sets.

(Zhao et al., 2025) introduces ARV-Q, an adaptive RISC-V vector processor offering unified support of PQC standards and side-channel security enhancement. The processor achieves 1.21-5.14× better latency than state-of-the-art counterparts and more than 4.41× better area efficiency through adaptive operator-type support and versatile Butterfly Units.

---

**Implementation Challenges and Real-World Deployment**

(Mamun et al., 2026) provides a comprehensive implementation-focused review addressing vulnerabilities at the physical implementation layer of cryptographic hardware, examining vulnerabilities in vehicular communication interfaces and IoT systems. The review identifies research gaps including non-PQC-ready standards, constraints in embedded implementation, interoperability barriers, and physical-attack vulnerabilities specific to PQC implementations.

**IV. SIDE-CHANNEL ATTACK ANALYSIS AND AI-DRIVEN DETECTION****Advanced Power and Electromagnetic Analysis**

(Tosun et al., 2025) develops efficient higher-order Correlation Power Analysis (HOCPA) attacks for lattice-based cryptography, introducing sin and cos prediction functions which prove optimal for HOCPA attacks against second and higher-order masking protection. The approach demonstrates full secret-key recovery from real devices with significantly reduced trace requirements through novel lattice reduction techniques combined with generic distinguishers.

(Jendral & Dubrova, 2026) presents the first side-channel security evaluation of VOLEitH-based signature schemes like FAEST, demonstrating two single-trace, deep learning-assisted power analysis attacks. These attacks exploit leakage from witness bits and VOLE tag computations, recovering the full secret key with success probability above 0.99 from a single signature on an ARM Cortex-M4 processor.

**AI-Driven Anomaly Detection Systems**

(Praditasari et al., 2025) introduces an unsupervised, resource-efficient anomaly detection framework tailored to post-quantum cryptography systems. The approach leverages an autoencoder trained solely on benign traces to learn deep latent representations of normal cryptographic behavior, achieving an average classification accuracy of 98.1% with a false positive rate of 0.7% and false negative rate of 0.4%, deployable on real-world PQC-enabled IoT systems.

(Ghubaish et al., 2024) proposes HDRL-IDS, a hybrid deep reinforcement learning IDS for enhancing security in 5G networks with Medical Internet of Things applications. The approach combines analysis of network and host features, leveraging advantages of both Network IDS (NIDS) and Host IDS (HIDS), outperforming traditional approaches in threat detection efficacy.

**Deep Learning for Trace Analysis**

(Tenentes et al., 2024) proposes an RTL flow for resilience assessment against power SCA attacks using deep learning-based SCA. The approach collects power traces considering resolution, sampling frequency, and measurement error, using deep learning to obtain guessing entropy metrics for Keccak-f implementations. Results identify characteristics making PQC designs vulnerable to power SCA attacks.

(Moos, 2020) evaluates physical security properties of unrolled cryptographic IC implementations through silicon measurements of an unrolled PRINCE core in 40nm ASIC. While unrolling provides intrinsic resistance to dynamic power analysis, the research reveals that static power consumption remains a critical attack vector, demonstrating that multiple power information leakage pathways exist in modern cryptographic circuits.

**Fault Injection and Timing Attacks**

(Amer et al., 2025) demonstrates Rowhammer-based attacks on NIST PQC finalists (Kyber, BIKE, and Dilithium), enabling complete key recovery with moderate effort. The practical feasibility of these attacks using Rowhammer, performance degradation, and memory massaging techniques demonstrates that such side-channel-based attacks remain critical concerns requiring implementation hardening.

(Liu et al., 2025) investigates the side-channel resistance of CRYSTALS-Dilithium by proposing a novel single-bit leakage attack that recovers target bits of large randomness used in the algorithm. Experiments on Cortex M4 demonstrate that the success rate of single-bit recovery can be improved by approximately 20% compared to existing state-of-the-art attacks.

## V. ETHICAL IMPLICATIONS AND SECURITY GOVERNANCE

### Dual-Use Concerns in Automated Vulnerability Discovery

The automation of vulnerability discovery through AI raises significant ethical concerns regarding dual-use applications. While automated testing enhances legitimate security practices, the same techniques could be weaponized by malicious actors. (Zhang, 2025) explores AI applications in cybersecurity, highlighting that AI is increasingly leveraged by malicious actors to automate attacks, significantly increasing their effectiveness and making detection more challenging. The research emphasizes the need for robust AI models resistant to adversarial attacks, increased algorithm transparency, and implementation of international AI regulation standards.

(Golikov & Ostrianska, 2024) discusses major risks associated with AI use in cybersecurity, including Data Poisoning attacks, Evasion Attacks, Prompt Injection Attacks, and AI-based social engineering. The study recommends developing robust AI models resistant to adversarial attacks, increased algorithm transparency, and implementation of international AI regulation standards including NIST guidance.

### Responsibility and Disclosure Practices

The development of automated attack discovery systems necessitates clear responsibility frameworks and ethical disclosure practices. Organizations deploying DRL-based vulnerability discovery must establish responsible disclosure protocols, working with affected parties to remediate discovered vulnerabilities before public disclosure. (Ohashi et al., 2024) proposes orthogonal adversarial deep reinforcement learning techniques for robust DRL, demonstrating that framework design choices significantly influence robustness properties and vulnerability to adversarial perturbations.

### Regulatory and Compliance Frameworks

(Kundu & Kompella, 2025) explores PQC-readiness and associated challenges, introducing algorithms for analyzing cryptography vulnerabilities through ciphersuite dependency graphs and cryptography bill of materials (CBOM) generation. The research emphasizes the importance of organizational cryptographic inventory, risk assessment, standards monitoring, and vendor engagement for compliance with emerging quantum-safe requirements.

(Aydeger et al., 2024) presents a comprehensive strategy for transitioning to post-quantum cryptography that encompasses identification, protection, detection, response, and recovery phases integrated with NIST Cybersecurity Framework Version 2.0. The roadmap emphasizes the importance of hybrid approaches, regulatory considerations, and coordinated strategies for quantum resilience.

### International Cooperation and Standards Development

International cooperation in cryptographic standardization, such as NIST's post-quantum cryptography initiative, represents critical infrastructure for establishing widely accepted quantum-safe cryptographic protocols. (Adapa, 2025) provides actionable insights for organizations preparing for the quantum computing era, emphasizing that successful transition requires a multi-faceted approach combining technical implementation with organizational readiness and strategic planning.

## VI. FUTURE DIRECTIONS AND RESEARCH CHALLENGES

### Integration of Hybrid Cryptographic Approaches

Future research must focus on seamless integration of classical and post-quantum cryptography. (Zoysa et al., 2025) presents a hybrid framework for quantum-resistant TLS handshakes integrating post-quantum cryptography, quantum key distribution, and classical cryptography to provide comprehensive protection against both classical and quantum attacks. The experimental implementation evaluated 144 distinct cryptographic protocol combinations, demonstrating optimal performance with ML-KEM combined with ML-DSA.

(Wang & Ismail, 2025) proposes a Hybrid Cryptographic Framework (HCF) integrating classical and quantum-resistant primitives, combining hybrid key exchange mechanisms, dual-signature schemes, and PQC-compatible

Merkle trees. The framework includes a discrete multi-objective optimization model to select algorithms meeting real-world constraints, facilitating a secure and interoperable transition.

### **Scalability and Performance Optimization**

Achieving scalable DRL-based vulnerability discovery requires addressing computational complexity and real-time deployment constraints. (Chen et al., 2024) demonstrates that deep reinforcement learning frameworks can achieve significant performance improvements in automated testing through advanced neural network architectures and prioritized experience replay. Future work must extend these approaches to more complex cryptographic implementations and larger attack surfaces.

(Rodriguez-Alvarez & Merino, 2025) evaluates Kyber's practical viability through performance testing utilizing only standard built-in processor acceleration features (AES-NI, ASIMD) without specialized hardware additions. The findings demonstrate that Kyber provides robust security guarantees against quantum attacks while maintaining acceptable performance profiles for contemporary applications.

### **Emerging Threats and Quantum-Era Challenges**

(Baseri et al., 2025) conducts a comprehensive risk assessment of quantum vulnerabilities across critical blockchain components using STRIDE threat modeling framework. The research provides actionable mitigation strategies, including quantum-resistant hash functions and PQC integration, while presenting hybrid blockchain architectures for secure migration with balance between security, adaptability, and operational efficiency.

(Kumar et al., 2025) analyzes the risks posed by quantum computing to classical cryptographic frameworks, evaluating quantum-resistant alternatives and highlighting the dangers of delayed PQC implementation. The research emphasizes the need for international cooperation, policy alignment, and robust testing to ensure effective deployment of quantum-resistant solutions for critical infrastructure.

### **Advanced Architectures and AI Integration**

(Dai et al., 2024) employs deep reinforcement learning to explore proficient quantum machine learning model architectures tailored for designated supervised learning tasks. The methodology demonstrates the efficacy of RL-driven approaches in discovering efficient QML models without predetermined ansatz, with adaptive mechanisms for dynamic learning objective adjustment.

(Gao et al., 2024) proposes Reinforcement Learning-based Causal Bayesian Experimental Design (RL-CBED) to reduce local optimality risk and accelerate intervention selection inference in causal discovery. The research proves that Q-function estimators can be learned using trajectories from the prior, significantly reducing training time costs and enabling real-world application of advanced RL methods.

## **VII. CONCLUSION**

This comprehensive research reveals that Deep Reinforcement Learning represents a transformative approach for automated vulnerability discovery in post-quantum cryptographic implementations. The integration of DRL with side-channel analysis enables identification of implementation flaws that traditional cryptanalysis often misses, achieving remarkable success rates in automated attack discovery.

However, significant challenges remain in bridging the gap between theoretical security guarantees of PQC algorithms and their practical implementations. Side-channel vulnerabilities persist despite ongoing countermeasure development, requiring continuous innovation in both defense and attack methodologies. The ethical implications of automated vulnerability discovery demand careful consideration of dual-use concerns and responsible disclosure practices.

Future research must prioritize scalable deployment of DRL-based security testing frameworks, seamless integration of hybrid cryptographic approaches, and robust governance structures ensuring that AI-driven cryptographic analysis advances security without enabling malicious exploitation. The transition to quantum-resistant cryptography requires coordinated international efforts, standards compliance, and continuous adaptation to emerging threats in the quantum computing era.

### VIII. REFERENCES

- [1] Adapa, V. R. K. (2025). Architecting quantum-resistant cybersecurity: A framework for transitioning to post-quantum cryptographic systems. International Journal of Science and Research Archive.
- [2] AlMajali, A., Al-Abed, L., Yousef, K. M. A., Mohd, B. J., Samamah, Z., & Shshadeh, A. A. (2024). Automated vulnerability exploitation using deep reinforcement learning. Applied Sciences.
- [3] Amer, S., Wang, Y., Kippen, H., Dang, T., Genkin, D., Kwong, A., Nelson, A., & Yerukhimovich, A. (2025). PQ-hammer: End-to-end key recovery attacks on post-quantum cryptography using rowhammer. IEEE Symposium on Security and Privacy.
- [4] Amouei, M., Rezvani, M., & Fateh, M. (2022). RAT: Reinforcement-learning-driven and adaptive testing for vulnerability discovery in web application firewalls. IEEE Transactions on Dependable and Secure Computing.
- [5] Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. International Conference on Network of the Future.
- [6] Baseri, Y., Hafid, A., Shahsavari, Y., Makrakis, D., & Khodaiemehr, H. (2025). Blockchain security risk assessment in quantum era, migration strategies, and proactive defense. IEEE Communications Surveys and Tutorials.
- [7] Beirendonck, M. V., D'Anvers, J.-P., Karmakar, A., Balasch, J., & Verbauwhede, I. (2021). A side-channel-resistant implementation of SABER. IACR Cryptology ePrint Archive.
- [8] Chen, J., Yan, L., Wang, S., & Zheng, W. (2024). Deep reinforcement learning-based automatic test case generation for hardware verification. Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023.
- [9] Cryptanalysis, Kumar, K., Durga, A., Kumar, P., Sundari, R., Ashwani, D., & Bilgaiyan, S. (2025). Automated cryptographic weakness discovery: A reinforcement learning approach for adaptive cryptanalysis. 2025 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC).
- [10] Dai, X., Wei, T.-C., Yoo, S., & Chen, S. Y. (2024). Quantum machine learning architecture search via deep reinforcement learning. International Conference on Quantum Computing and Engineering.
- [11] Ezeogu, A. (2025). POST-QUANTUM CRYPTOGRAPHY FOR HEALTHCARE: FUTURE-PROOFING POPULATION HEALTH DATABASES AGAINST QUANTUM COMPUTING THREATS. Research Corridor Journal of Engineering Science.
- [12] Fritzmann, T., Beirendonck, M. V., Roy, D. B., Karl, P., Schamberger, T., Verbauwhede, I., & Sigl, G. (2021). Masked accelerators and instruction set extensions for post-quantum cryptography. IACR Cryptology ePrint Archive.
- [13] Gao, H., Sun, Z., Yang, H., & Chen, X. (2024). Policy-based bayesian active causal discovery with deep reinforcement learning. Knowledge Discovery and Data Mining.
- [14] Ghubaish, A., Yang, Z., & Jain, R. (2024). HDRL-IDS: A hybrid deep reinforcement learning intrusion detection system for enhancing the security of medical applications in 5G networks. International Conference on Smart Communications and Networking.
- [15] Golikov, Y., & Ostrianska, Y. (2024). RESEARCH ON THE CURRENT STATE AND PROSPECTS OF THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY. Computer Science and Cybersecurity.
- [16] Hore, S., Shah, A., & Bastian, N. D. (2022). Deep VULMAN: A deep reinforcement learning-enabled cyber vulnerability management framework. Expert Systems with Applications.
- [17] Jendral, S., & Dubrova, E. (2026). Side-channel attacks on VOLEith signature schemes: Breaking masked FAEST. IACR Commun. Cryptol.
- [18] Kasture, S., Maurya, S., Singh, A., Shukla, A., Kotiyal, A., & Mirza, K. (2025). Securing post-quantum cryptography: Side-channel resilience in CRYSTALS-kyber key encapsulation mechanism. IAES International Journal of Artificial Intelligence (IJ-AI).
- [19] Kim, B. D., Vasudevan, V. A., D'Oliveira, R. G. L., Cohen, A., Stahlbuhk, T., & M'edard, M. (2025). Cryptanalysis via machine learning based information theoretic metrics. arXiv.org.

- [20] Kumar, S., Klappenecker, A., Brown, G., & Saravanan, S. (2025). Quantum apocalypse: Fortifying critical infrastructure in the age of cyber warfare. European Conference on Cyber Warfare and Security.
- [21] Kundu, A., & Kompella, R. (2025). Quantum-resistant security: PQC readiness and research challenges (invited). Design Automation Conference.
- [22] Liu, B., Zhang, J., & Wang, A. (2025). Single bit randomness leakage: The vulnerability in post-quantum cryptography standard CRYSTALS-dilithium. International Congress on Information and Communication Technology.
- [23] Mamun, A. A., Abrar, A., Rahman, M., Salek, M., & Chowdhury, M. (2026). Post-quantum cryptography for intelligent transportation systems: An implementation-focused review. arXiv.org.
- [24] Marin, F., Arduin, P.-E., & Merad, M. (2025). Physics-informed graph neural networks for attack path prediction. Journal of Cybersecurity and Privacy.
- [25] McFadden, S., Maugeri, M., Hicks, C., Mavroudis, V., & Pierazzi, F. (2024). WENDIGO: Deep reinforcement learning for denial-of-service query discovery in GraphQL. 2024 IEEE Security and Privacy Workshops (SPW).
- [26] Moos, T. (2020). Unrolled cryptography on silicon a physical security analysis. IACR Trans. Cryptogr. Hardw. Embed. Syst.
- [27] Obaid, Z. M., & Alheeti, K. (2023). Comprehensive study of side-channel analysis (CyberSecurity). International Conference on Developments in eSystems Engineering.
- [28] Ohashi, K., Nakanishi, K., Goto, N., Yasui, Y., & Ishii, S. (2024). Orthogonal adversarial deep reinforcement learning for discrete- and continuous-action problems. IEEE Access.
- [29] Praditasari, W. A., Kim, H., Yoon, H., Rimbawa, D., & Yi, O. (2025). AI-driven defense mechanism for lattice-based post-quantum cryptography: Adaptive mitigation against side-channel attacks. Asia Joint Conference on Information Security.
- [30] Qiao, Z., Liu, Y., Zhou, Y., Zhao, Y., Yuan, H., & Du, D. (2025). Efficient CNN-based side-channel attacks on dilithium without device access. International Symposium on Circuits and Systems.
- [31] Rane, S. R. (2025). Quantum-resistant cryptographic algorithms: A comparative analysis for securing next-generation communication networks. Journal of Information Systems Engineering & Management.
- [32] Ravi, P., Chattopadhyay, A., D'Anvers, J.-P., & Baksi, A. (2023). Side-channel and fault-injection attacks over lattice-based post-quantum schemes (kyber, dilithium): Survey and new results. IACR Cryptology ePrint Archive.
- [33] Rodriguez-Alvarez, N., & Merino, F. (2025). Performance and storage analysis of CRYSTALS kyber as a post quantum replacement for RSA and ECC. arXiv.org.
- [34] Tenentes, V., Matteo, S., Zonios, C., Rossi, D., & Saponara, S. (2024). RTL flow for the power side-channel resilience assessment of a post-quantum SHA-3 accelerator. International Conference on Modern Circuits and Systems Technologies.
- [35] Tosun, T., Oswald, E., & Savaş, E. (2025). Non-profiled higher-order side-channel attacks against lattice-based post-quantum cryptography. IACR Cryptology ePrint Archive.
- [36] V, S. B., A, A., & Naval, P. (2023). Deep reinforcement learning in automated network vulnerability detection. 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET).
- [37] Wang, Y., & Ismail, E. S. (2025). A review on the advances, applications, and future prospects of post-quantum cryptography in blockchain and IoT. IEEE Access.
- [38] Zhang, C. (2025). Research progress on network security threat detection and defense technology based on artificial intelligence. Applied and Computational Engineering.
- [39] Zhao, Y., Kuang, H., Yu, X., Sun, Y., Hao, Z., Meng, J., & Han, J. (2025). ARV-q: An adaptive RISC-v vector processor for unified support of post-quantum standards and side-channel protection on the edge. IEEE Transactions on Circuits and Systems Part 1: Regular Papers.
- [40] Zoysa, D. D., Perera, M., & Weerasinghe, H. (2025). A hybrid framework for quantum-resistant TLS handshakes with PQC, QKD and classical cryptography. 2025 International Conference on Advances in Technology and Computing (ICATC).